REMARKS

The Office Action dated July 23, 2008, has been received and carefully noted. The above amendments to the specification and claims, and the following remarks, are submitted as a full and complete response thereto.

By this Response, claims 1-5, 8, 10, 13-15, and 17-20 have been amended to more particularly point out and distinctly claim the subject matter of the present invention. Claims 11-12 and 21-22 have been cancelled without prejudice or disclaimer. Claims 23-69 have been added. No new matter has been added. Support for the above amendments is provided in the Specification at least on pages 14-24. Accordingly, claims 1-10, 13-20, and 23-69 are currently pending in the application, of which claims 1, 18, 26, 36, 47, 57, and 67-69 are independent claims.

In view of the above amendments and the following remarks, Applicants respectfully request reconsideration and timely withdrawal of the pending rejections to the claims for the reasons discussed below.

Abstract and Specification

The Office Action objected to the Abstract, stating that it includes "means" phrases and exceeds 150 words. Further, the Office Action objected to the disclosure of the Specification because the Specification allegedly failed to layout the sections of the Specification as required by 37 C.F.R. §1.77(b).

Accordingly, Applicants submit with this Response a substitute Specification and Abstract, rendering the objections to the Abstract and Specification moot.

Therefore, Applicants respectfully request withdrawal of the objections to the Abstract and the disclosure of the Specification, and respectfully submit that the Abstract and the Specification are now in condition for issuance.

Claim Objections

The Office Action objected to claims 18-20 because of minor informalities. Specifically, the Office Action alleged that in claims 18-20 the phrase "arranged to" is not a positive limitation and does not constitute a limitation in any patentable sense.

Accordingly, Applicants have amended claims 18-20 to replace "arranged to" with "configured to," as recommended in the Office Action, rendering the objections to claims 18-20 moot.

Therefore, Applicants respectfully request withdrawal of the objection of claims 18-20, and respectfully submit that claims 18-20 are now in condition for allowance.

Claim Rejections under 35 U.S.C. §101

The Office Action rejected claim 18 under 35 U.S.C. §101 as allegedly directed to a method that does not produce a useful, concrete, and tangible result, *i.e.* the claim is allegedly directed to non-statutory subject matter.

Applicants note that claim 18 recites features for a *system* claim. Accordingly, Applicants respectfully disagree with the Office Action's conclusions that claim 18 is directed to a method. To further clarify the features of the system recited in claim 18, Applicants have amended claim 18 to more particularly point out and distinctly claim the subject matter of the system, rendering the rejection of claim 18 under 35 U.S.C. moot.

Therefore, Applicants respectfully request withdrawal of the rejection of claim 18 under 35 U.S.C. §101, and submit that claim 18 is now in condition for allowance.

Claim Rejections under 35 U.S.C. §102(e)

The Office Action rejected claims 1-20 under 35 U.S.C. §102(e) as allegedly being anticipated by Green, *et al.* (U.S. Patent Publication No. 2004/0015692) ("Green"). The Office alleged that Green discloses or suggests each and every element recited in claims 1-20. Applicants respectfully submits that the claims recite subject matter that is neither disclosed nor suggested in Green.

Claim 1, upon which claims 2-17 and 20 depend, recites a method. The method includes executing an authentication protocol. The terminal authentication protocol includes authenticating an identity of a network entity by a terminal in a communication system, and sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity. The method further includes executing another authentication protocol. The another authentication protocol includes sharing challenge data between the network entity and the terminal, and

forming at the terminal test data by applying an authentication function to the challenge data. The another authentication protocol further includes sending a message comprising terminal authentication data, from the terminal to the network entity, and determining, based on the terminal authentication data, whether to provide the terminal with access to a service. The determining includes providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key.

Claim 18, upon which claim 19 depends, recites a system. The system includes a terminal configured to apply authentication functions to input data to form response data, and a network entity configured to provide access to a service. The system is configured to perform an authentication method of executing an authentication protocol. The authentication protocol includes authenticating an identity of the network entity by the terminal in the system, and sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity. The authentication protocol further includes executing another authentication protocol. The another authentication protocol includes sharing challenge data between the network entity and the terminal, and forming at the terminal test data by applying an authentication function to the challenge data. The another authentication protocol further includes sending a message comprising terminal authentication data from the terminal to the network entity, and determining, based on the terminal authentication data, whether to provide the terminal with access to a service. The determining includes providing the

terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key.

As will be discussed below, Green fails to disclose or suggest each and every element recited in claims 1-20, and therefore fails to provide the features discussed above.

Green is directed to an authentication in a mobile communications network. The network includes an authenticating a subscriber identifying means to a network entity and authenticating a network entity to the subscriber identifying means (Green, Abstract).

Applicants respectfully submit that Green fails to disclose or suggest each and every element recited in claims 1 and 18. In particular, Green fails to disclose or suggest, at least, "sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity; and executing another authentication protocol comprising sharing challenge data between the network entity and the terminal; forming at the terminal test data by applying an authentication function to the challenge data; sending a message comprising terminal authentication data, from the terminal to the network entity; and determining, based on the terminal authentication data, whether to provide the terminal with access to a service, wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key," as recited in claim 1 (emphasis added), and similarly recited in claim 18.

Rather, Green relates to preventing a malicious person from repeatedly sending random numbers as authentication challenges to a SIM and to monitoring the signed responses. Hence, Green is directed to preventing a multiple attack (Green, paragraphs [0008]-[0009]).

As illustrated in Figures 3a, 3b, and 3c, Green describes a process of mutual authentication. Green teaches that challenge information is sent from a mobile switching center to a terminal. The challenge information includes RAND and CERT. The terminal calculates CERT from a key and depending on whether the value CERT is correct, replies with either a false response or a correct response (Green, paragraphs [0085]-[0086]).

However, Green fails to mention *sharing* authentication keys. Rather, as described in paragraph [0006], Green describes that the authentication key K_i is stored on a SIM in a very *protected* way. Accordingly, it is not possible to share the authentication key K_i because it is secured. Therefore, one of ordinary skill in the art would understand that Green fails to disclose or suggest *a sharing of the authentication key.*

Furthermore, Green teaches that in response to receiving the challenge information (*e.g.*, RAND), a response SRES is sent back to the MSC. SRES is calculated from K, however, since K cannot be shared, SRES is *not* a predetermined function of a *shared key* and test data.

For the Examiner's convenience, it is noted that, as described at page 16, step 76, of the original specification a session key T can be shared. This is different from key K which may be secure (see page 13 of the original specification).

Furthermore, Green fails to mention "man in the middle" attacks, and therefore, one of ordinary skill in the art would not have been motivated to look to the teachings of Green. Certain embodiments of the present invention use an existing challenge response protocol for a two stage authentication function to overcome the potential vulnerability of a "man in the middle" attack. Green does not even mention addressing this problem.

Therefore, Green fails to disclose or suggest, at least, "sharing a key between the terminal and the network entity for use in securing subsequent communications between the terminal and the network entity...wherein the determining comprises providing the terminal with access to the service only when the terminal authentication data equals a predetermined function of at least the test data and the key," as recited in claim 1, and similarly recited in claim 18.

Claims 2-17 depend from claim 1. Claim 19 depends from claim 18. Accordingly, claims 2-17 and 19 should be allowable for at least their dependency upon an allowable base claim, and for the specific limitations recited therein.

Therefore, Applicants respectfully request withdrawal of the rejections of claims 1-20 under 35 U.S.C. §102(e) and respectfully submit that claims 1 and 18, and the claims that depend therefrom, are now in condition for allowance.

CONCLUSION

In conclusion, Applicants respectfully submit that Green fails to disclose or suggest every feature recited in claims 1-10, 13-20, and 23-69. The distinctions

previously noted are more than sufficient to render the claimed invention unanticipated. It is therefore respectfully requested that all of claims 1-10, 13-20, and 23-69 be allowed, and this present application be passed to issuance.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Peter Flanagan #58,178

Brad Y. Chin
Attorney for Applicants
Registration No. 52,738

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

BYC:dlh

Enclosures: Marked-Up Copy of Substitute Specification and Abstract
Clean Copy of Substitute Specification and Abstract
Additional Claim Fee Transmittal
Check No. 000019901